

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
29 June 2006 (29.06.2006)

PCT

(10) International Publication Number
WO 2006/068450 A1

(51) International Patent Classification:
H04B 7/26 (2006.01)

(21) International Application Number:
PCT/KR2005/004503

(22) International Filing Date:
23 December 2005 (23.12.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
1433/CHE/2004 24 December 2004 (24.12.2004) IN

(71) Applicant (for all designated States except US): **SAM-SUNG ELECTRONICS CO., LTD.** [KR/KR]; 416, Maetan-dong, Yeongtong-gu, Suwon-si, Gyeonggi-do 442-742 (KR).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **BALAJI, Holur** [IN/IN]; J.P. Techno Park, 3/1, Millers Road, Bangalore 560 052 (IN). **RAHUL, Vaidya** [IN/IN]; J.P. Techno Park, 3/1, Millers Road, Bangalore 560 052 (IN). **RA-JAVELSAMY, R** [IN/IN]; J.P. Techno Park, 3/1, Millers Road, Bangalore 560 052 (IN). **VENKATESWAR, J** [IN/IN]; J.P. Techno Park, 3/1, Millers Road, Bangalore

560 052 (IN). **SONG, O-Sok** [KR/KR]; #304-105, Hyundai Riverville APT., Pungnap 2-dong Songpa-gu, Seoul 138-042 (KR).

(74) Agent: **LEE, Keon-Joo**; Mihwa Bldg. 110-2, Myongryun-dong 4-ga, Chongro-gu, Seoul 110-524 (KR).

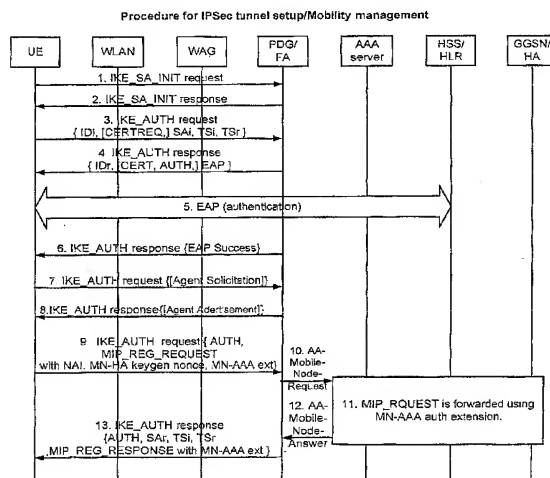
(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— with international search report

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR PROVIDING MOBILITY AND SECURE TUNNEL USING MOBILE INTERNET PROTOCOL WITHIN INTERNET KEY EXCHANGE PROTOCOL VERSION 2



(57) Abstract: The present invention is related to the scenario where a roaming MN needs to connect to NGW for establishing secure data path using IPsec procedure. Also MIP is used to support the mobility of the MN. However, when the Home Address of the MN is not known, a cyclic interdependency is observed between the IPsec procedures and MIP procedures. This happens as the IPsec procedure requires Home Address, and the MIP requires IPsec tunnel for transmitting the messages. The initial request for any PS service is by initiating an IPsec tunnel establishment request (IKEv2 procedure) with the NGW. After the authentication procedure within the IKEv2 protocol is over, the MN transmits the MIP registration messages within the IKEv2 message to the NGW. After the Mobile IP Registration is completed, the Home Address of the MN is known from the MIP registration Reply. MN forms a secured tunnel with the NGW.

WO 2006/068450 A1



For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

- 1 -

**SYSTEM AND METHOD FOR PROVIDING MOBILITY AND
SECURE TUNNEL USING MOBILE INTERNET PROTOCOL WITHIN
INTERNET KEY EXCHANGE PROTOCOL VERSION 2**

BACKGROUND OF THE INVENTION

FIELD OF THE INVENTION

This invention relates in general to mobile communications technology. Specifically, it is related to Mobility and creation of secure tunnel between Mobile Node (MN) and Network Gateway (NGW). More particularly, this invention provides a system and method to support mobility and secure tunnel creation, when the Home Address of the MN is not known while MN request for the Packet Switched (PS) service in the foreign network. The scope of the invention also covers the case when Home address as well as Home Agent address and Home network prefix of the MN are not known.

DESCRIPTION OF THE RELATED ART

The Mobility and the secure tunnel establishment procedure for the scenario as depicted in Figure 1 works as below:

When the MN roams in a foreign network, the MN forms a tunnel with the NGW to obtain Packet Services provided by the network. This can be done for example, to provide secure access over an untrusted interface (e. g. air interface with inadequate security).

The foreign network can provide a Local IP address to the MN (Local IP Address is routable only upto NGW) while the Remote IP address through which the MN is accessible to outside world is to be provided by the external network to which MN is trying to reach for the service (in this case we assume home network obtains the IP address from the external network and sends it to the MN).

MIP is used for providing mobility services when a mobile roams from one (sub) network to another (sub) network. MIP requires a node in the foreign network acting as a foreign agent, and a node in home network acting as a Home Agent. When an MN roams into a foreign network, it sends a registration request through the Foreign Agent to the Home Agent, indicating that it is available at the given IP address.

- 2 -

When the MN requires a new service:

1. The IP address of the NGW which provides the service is obtained by DNS query or by some other means. IKEv2 messaging is carried out between the MN and NGW (with optional authentication) to establish the IPsec SAs. At the end of the IKEv2 signaling a tunnel is formed between the MN and the NGW which acts as a data path.

2. Once the tunnel is formed MIP Registration request is sent to the Home Agent through FA. HA sends the Registration reply. If successful, the UE can now securely receive packets destined to it even when it roams in different foreign network.

Currently there is no mechanism for the following features:

To provide IPsec and mobility related scenario if the Home Address of the MN is unknown

Cyclic interdependency of IPsec tunnel formation and MIP Registration Signaling.

SUMMARY OF THE INVENTION

The primary object of the invention is to define an extension to the IKEv2 protocol to carry MIP messages to support mobility.

It is another object of the invention to define a method to break the cyclic interdependency between requirement of Remote IP address for IPsec SA (which can be obtained from MIP Registration process) and the requirement of IPsec SA between the NGW and the MN for transporting the MIP Registration Request messages.

It is another object of this invention to specify the IKEv2 message extensions to carry the MIP messages used during the procedure.

This invention provides a system and method to perform Mobility using IKEv2 extensions to carry MIP messages. By incorporating MIP messages within IKEv2 protocol, this invention provides the ability to solve the cyclic interdependency between requirement of Remote IP address (Home Address) for IPsec SA and the requirement of IPsec SA between NGW and the MN for transporting the Mobile IP (MIP) Registration Request messages.

Consider a scenario where the Mobile Node roams to a foreign network which does not provide adequate over the air security. Also consider that NGW

- 3 -

is a trusted entity either in foreign network or in home network. NGW provides secure path to any node in the home network. Thus, to provide secure communication channel between MN and home network, we consider forming an IPsec tunnel between MN and NGW.

5 The present invention enables the MN to:

- Roam while keeping the sessions alive;
- Provide security to MIP messages even when the Home Address of the MN is not known;

10 The present invention relates to a system that needs to form an IPsec tunnel with a foreign entity NGW. The invention also relates to a system that requires performing the MIP registration for mobility services. Further, this invention provides mechanisms for the case where the Home Address of the MN is not
15 known and the MN requests for the PS service in the foreign network.

20 The system for the invention comprises of an MN capable of roaming in foreign networks, Network Gateway, Foreign Agent in the foreign network (might or might not be collocated with NGW) and a Home Agent (HA) in home network.

The present invention comprises of system and method which would solve the problems associated with current art, as mentioned below.

25 The MN forms the tunnel with NGW. (Though we assume IKEv2 is used to establish the tunnel, any similar protocol may be used for the tunnel establishment).

30 The MIP messages are carried during the tunnel establishment within the IKEv2 messages and are passed to the Home Agent through the NGW and FA (if the FA is not co-located with the NGW).

35 If the MIP registration is successful, the HA sends the MIP Registration Reply containing the Home Address of the MN, which is relayed by the FA after registering the MN in its visitor's cache, to the NGW. The NGW forwards it to the MN within the IKE_AUTH message of the IKEv2 protocol to the MN. The MN can extract the Home IP address and the Home Agent address from the MIP Registration reply message.

The MN and the NGW now established the tunnel by configuring the IPsec SA from the IKE_AUTH message (of IKEv2) using Home IP address of the MN.

- 4 -

Accordingly, the present invention comprises a method for providing mobility and establishing a secure tunnel using IKEv2 messages and MIP messages between the Mobile Node (MN) or user equipment (UE) and the Network Gateway (NGW).

Accordingly, the present invention further comprises a system for providing mobility and establishing a secure tunnel using IKEv2 messages and MIP messages between the Mobile Node (MN) or user equipment (UE) and the Network Gateway (NGW) wherein the said system comprises of a MN capable of IPsec and MIP procedures, Network Gateway contained in either foreign network or home network, foreign agent collocated with NGW, and a Home Agent in the home network.

The other objects, features and advantages of the present invention will be apparent from the ensuing detailed description of the invention taken in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 illustrates the different network elements of the system considered in the invention.

Figure 2 illustrates the different network elements of a WLAN-3G interworking system, involved in establishing an End-To-End tunnel and Mobility support between UE and PDG.

Figure 3 illustrates the sequence for establishing the IPsec tunnel and MIP registration, when the Home Address is not known and the FA and the NGW are co-located.

DETAILED DESCRIPTION OF EXEMPLARY EMBODIMENTS

A preferred embodiment of the present invention will now be explained with reference to the accompanying drawings. It should be understood however that the disclosed embodiment is merely exemplary of the invention, which may be embodied in various forms. The following description and drawings are not to be construed as limiting the invention and numerous specific details are described to provide a thorough understanding of the present invention, as the basis for the claims and as a basis for teaching one skilled in the art how to make and/or use

- 5 -

the invention. However in certain instances, well-known or conventional details are not described in order not to unnecessarily obscure the present invention in detail.

5 The present invention provides a system and method for supporting mobility of the MN which requires the secured tunnel to communicate over and uses MIP protocol to support the mobility.

10 The method of the invention comprises of the mechanisms to break the cyclic interdependency between requirement of Home IP address of the MN for IPsec SA and the requirement of IPsec SA between NGW and MN for transporting the MIP Registration. When the MN access foreign network initially, it has no Home address. But the Home IP Address of the MN is essential to establish IPsec tunnel between the MN and the NGW and to tunnel all the packets to and from the MN
15 by the NGW. Therefore the described method comprises a mechanism to allocating a Home Address to the MN during the IPsec tunnel setup.

20 To obtain a Home IP address from the HA, the IKEv2 protocol is extended to carry the MIP messages from the MN to the NGW. The NGW extracts the MIP messages and forwards to the FA. The FA forwards the MIP message to the AAA server for authentication and to obtain the IP address of the MN from the HA and relays the MIP Registration Reply to the NGW and the NGW forwards it within the IKE_AUTH response message. Also the FA registers the UE in the visitor's cache according to the normal MIP protocol (According to IETF RFC).

25 One assumption using Mobile-AAA Authentication extension is that the MN and the AAA server share AAA Security Association. In this document, it is assumed that the MN and the AAA server share at least one AAA Security Association. It is also assumed that an AAA Security Association between the MN and the AAA server is dynamically created or updated after the AAA server authenticates the MN using EAP method during the IPsec tunnel setup
30 (According to IETF EAP Procedures). The shared secret of this AAA Security Association is any key derived from the Master Key after the IKEv2 authentication as a result of EAP procedure with in the IKEv2.

35 The operation of the invention is detailed below:

**Establishment of Tunnel and MIP Registration between MN and NGW
using MIP messages within the IKEv2 Messages**

- 6 -

When an MN needs to access a service provided by the network, it needs to form a tunnel with an NGW which can provide the service. The IP address of the NGW can be found by DNS query or by some other means.

MN initiates a tunnel establishment request with the NGW. As a part of the tunnel establishment, the user can be authenticated and authorized for the service.

[Optional] After the EAP authentication procedure within IKEv2, Mobile Agent Solicitation and Advertisement can be exchanged within the IKEv2 messages.

The MIP Registration message is passed within the IKEv2 messages from the MN to the NGW. The MIP registration message can include the NAI, MN_HA keygen nonce, MN_AAA authentication extensions (if the home agent address and home network prefix are not known).

The NGW extracts the MIP Registration message and forwards it to the FA, if the FA and the NGW are not co-located. Then the MIP Registration message is processed normally at FA and forwarded to AAA server. The AAA server process the MIP Registration request as like normal MIP protocol and forwards it to HA, which can serve the MN.

The HA sends the Mobile IP Registration Reply with the Home Address, if registration is successful, to the FA. The FA processes the registration reply message and registers the MN in its visitor's cache. The FA then forwards the MIP registration replay to the NGW, if the FA and the NGW are not co-located.

The NGW relays the MIP Registration reply message within the IKE_AUTH reply message of IKEv2 to the MN, with the TS and SA payloads to form the IPsec SA between the MN and the NGW, with the Home IP address of the MN.

On receiving the Registration Reply within the IKE_AUTH reply message of IKEv2, MN extracts the Home Address. Also it creates a new SA with the Home IP address. Thus the data path to the network is created.

An illustrative Example for the operation of the invention:

A 3G-WLAN interworking scenario is considered here. The 3GPP (<http://www.3gpp.org>) specification TS23.234, which deals with the ongoing 3GPP work related to WLAN-3G interworking, provides a system description for tunnel establishment mechanism between WLAN-3G UE and PDG over a WLAN-3G interworking system, as depicted in Figure 2. The different network elements of a WLAN-3G interworking system, involved in establishing an End-To-End tunnel and Mobility support between UE and PDG is shown in **Figure 2** function as below:

- 7 -

WLAN UE – User Equipment, to initiate the tunnel for data path.

WLAN – to pass the EAP signaling and data packets towards the 3G-WLAN network.

WAG – Wireless Access Gateway, to enforce the policies and filters on WLAN AN.

PDG – Packet Data Gateway, A 3G-WLAN Interworking, network entity that serves as the gateway between a WLAN AN and PDNs. The PDG allows 3G-WLAN users to access PDNs.

GGSN – Gateway GPRS Support Node. A GPRS network entity that serves as the mobile wireless gateway between an SGSN and PDNs. The GGSN allows mobile users to access PDNs.

SGSN – Serving GPRS Support Node. A GPRS network entity that sends data to and receives data from mobile stations, and maintains information about the location of an MS. The SGSN communicates between the MS and the GGSN; the GGSN provides access to the data network

UTRAN - UMTS Terrestrial Radio Access Network, air interface portion of UMTS networks as specified within 3GPP.

AAA Server - Authentication, Authorization, and Accounting server to intelligently controlling access, enforcing policies, auditing usage, and providing the information necessary to do billing for services available through the 3G-WLAN Interworking Network.

HSS and HLR - Home Subscriber Server and Home Location Register, to have subscriber credentials and details

CCF and OCS – Call Control function and Open Card Framework for billing and call control

In comparison to the above mentioned invention, the PDG here acts as a Network Gateway which resides in the foreign network, i.e. the Foreign Agent is collocated with the PDG for the sake of simplicity, although it is not necessary for this invention to work. The Home Agent is assumed to be collocated with GGSN of 3G network for the sake of simplicity, although it is not necessary for this invention to work. The scenario considered here is when the WLAN UE needs to access some PS service. The UE does not know Home Address and Home Agent Address.

The example shows the FA to co-exist with PDG, though it is not mandatory. The following steps briefly explain the operation of the example for the system architecture shown in Figure 2. The message flows/sequence illustrated in **Figure 3** is as below:

- 8 -

1 and 2. The UE and the PDG negotiate IKE_SA.

3. The UE sends IKE_AUTH request, without AUTH payload to initiate EAP procedure. The IDi payload in IKE_AUTH request must contain the NAI of the UE. Optionally, the UE can attach CERTREQ payload to the IKE_AUTH request if it wants to authenticate the PDG using signature based authentication. The TSr payload contains 0.0.0.0/0 (indicating full range of IP address from 0.0.0.0 to 255.255.255.255).

4. PDG sends EAP Request/ID in IKE_AUTH message, initiates the EAP authentication procedure.

5. UE responds with EAP Response ID in IKE_AUTH, initiation of EAP is optional. The PDG sends an Access Request [NAI] to AAA server. The NAI is obtained from IDi field in IKE_AUTH message. The AAA server retrieves Authentication Data and User profile informations from HSS/HLR. AAA responds with Access Response [EAP-AKA/challenge]. PDG forwards the EAP-AKA/Challenge to UE in IKE_AUTH message. It's optional to include [CERT, AUTH] in the message. Normal EAP authentication is carried on between UE and AAA with PDG/FA acting as a relay agent. When all checks are successful, the AAA server sends an EAP success and the key material to the PDG.

6. The PDG forwards only the EAP success message within the IKEv2 message to the UE.

7 and 8. [Optional] Mobile Agent Solicitation and Advertisement can be exchanged within the IKEv2 messages.

9. The UE sends IKE_AUTH response that contains AUTH payload. The UE uses shared secret derived from EAP authentication procedure to make AUTH payload. UE also includes MIP REGISTRATION REQUEST with NAI, MN_HA keygen nonce and MN_AAA authentication extensions.

10. On receiving the MIP message, PDG forwards it to the FA (whose IP address is mentioned as CoA in MIP). The FA sends the MIP-Registration-Request to AAA in appropriate AAA messages.

- 9 -

11. AAA server, after authenticating the UE, generates keys as requested in registration message, and distributes to the respective agents. FA can then forward the Registration Request to the HA, if it has not relayed it earlier.

5 12. HA then sends the Registration Reply to the FA. The FA then registers the UE in its visitor's cache and forwards the registration reply to the PDG, if the PDG and the FA are not co-located.

10 13. The PDG sends IKE_AUTH response that contains AUTH payload. The PDG makes AUTH payload with the shared secret derived from EAP authentication procedure. It also includes the MIP REGISTRATION REPLY. The TSi in the IKE_AUTH message contains the Home Address of the UE as the IP parameter.

15 The UE obtains the Home Address from the MIP_REG_REPLY and completes the tunnel establishment procedure.

20 As stated previously, the above procedure can be applied to the 3G-WLAN case, where the Network gateway is PDG, and HA is collocated with GGSN (or is in the same sub-network).

The user authentication is carried out by RADIUS/Diameter messages between the PDG and AAA server in the home network.

25 The PDG IP address can be discovered in the network by using DNS query over the W-APN. W-APN is the indicative of the service required by the WLAN-UE. The DNS reply contains the list of PDGs capable of providing the given service.

30 It will also be obvious to those skilled in the art that other control methods and apparatuses can be derived from the combinations of the various methods and apparatuses of the present invention as taught by the description and the accompanying drawings and these shall also be considered within the scope of the present invention. Further, description of such combinations and variations is therefore omitted above. It should also be noted that the host for storing the
35 applications include but not limited to a computer, mobile communication device, mobile server or a multi function device.

- 10 -

Although the present invention has been fully described in connection with the preferred embodiments thereof with reference to the accompanying drawings, it is to be noted that various changes and modifications are possible and are apparent to those skilled in the art. Such changes and modifications are to be understood as included within the scope of the present invention as defined by the appended claims unless they depart there from.

5

- 11 -

WHAT IS CLAIMED IS:

1. A method for providing mobility and establishing a secure tunnel using IKEv2 messages and MIP messages between the Mobile Node (MN) or user equipment (UE) and the Network Gateway (NGW).

2. A method as claimed in claim 1 wherein the said method break the cyclic interdependency between requirement of Home Address for IPsec SA and the requirement of IPsec SA between NGW and MN for transporting the MIP Registration Request messages.

3. A method as claimed in claim 2 wherein the Home IP Address of the MN essential to establish IPsec tunnel between the MN and the NGW is obtained comprising the steps of:

the IKEv2 protocol extending to carry the MIP messages from the MN to the NGW;

extracting the MIP messages and forwards to the FA by NGW;

forwarding the MIP message to the AAA server for authentication by FA;

obtaining the IP address of the MN from the HA and relaying the MIP Registration Reply to the NGW ;

forwarding within the IKE_AUTH response message by NGW; and

registering the UE in the visitor's cache according to the normal MIP protocol by FA .

4. A method as claimed in claim 1 wherein the said method defines an extension to the IKEv2 protocol to carry MIP messages to support mobility while establishing the tunnel.

5. A method as claimed in claim 1 wherein for establishment of Tunnel and MIP Registration, MN needs to access a service provided by the network where it needs to form a tunnel with a NGW which can provide the service and the IP address of the NGW can be found by DNS query or by some other means.

6. A method as claimed in claim 5 wherein MN initiates a tunnel establishment request with the NGW and the user is authenticated and authorized for the service.

- 12 -

7. A method as claimed in claim 6 wherein after the authentication procedure within IKEv2, Mobile Agent Solicitation and Advertisement is exchanged within the IKEv2 messages.

5 8. A method as claimed in claim 7 wherein the MIP Registration message is passed within the IKEv2 messages from the MN to the NGW and the MIP registration message include the NAI, MN_HA keygen nonce, MN_AAA authentication extensions if the home agent address and home network prefix are not known.

10 9. A method as claimed in claim 8 wherein the NGW extracts the MIP Registration message and forwards it to the FA, if the FA and the NGW are not co-located then the MIP Registration message is processed normally at FA and forwarded to AAA server where AAA server process the MIP Registration
15 request as like normal MIP protocol and forwards it to HA, which can serve the MN.

20 10. A method as claimed in claim 9 wherein the HA sends the Mobile IP Registration Reply with the Home Address, if registration is successful, to the FA where the FA process the registration reply message and registers the MN in its visitor's cache and the FA then forwards the MIP registration reply to the NGW, if the FA and the NGW are not co-located.

25 11. A method as claimed in claim 10 wherein the NGW relays the MIP Registration reply message within the IKE_AUTH reply message of IKEv2 to the MN, with the TS and SA payloads to form the IPsec SA between the MN and the NGW, with the Home IP address of the MN.

30 12. A method as claimed in claim 11 wherein on receiving the Registration Reply within the IKE_AUTH reply message of IKEv2, MN extracts the Home Address and creates a new SA with the Home IP address thus creating the data path to the network.

35 13. A method as claimed in claim 1 wherein the said method is utilized for tunnel establishment mechanism between WLAN-3G UE and PDG over a WLAN 3G interworking system comprising the steps of:

negotiating IKE_SA by UE and the PDG;
sending IKE_AUTH request, without AUTH payload to initiate EAP procedure by UE;

- 13 -

PDG sending EAP Request/ID in IKE_AUTH message whereby initiates the EAP authentication procedure;

UE responding with EAP Response ID in IKE_AUTH;

PDG forwarding the EAP success message within the IKEv2 message to the UE;

Mobile Agent Solicitation and Advertisement exchanging within the IKEv2 messages;

UE sending IKE_AUTH response that contains AUTH payload;

On receiving the MIP message, PDG forwarding it to the FA;

FA sending the MIP-Registration-Request to AAA in appropriate AAA messages;

AAA server, after authenticating the UE, generating keys as requested in registration message, and distributes to the respective agents;

FA forwarding the Registration Request to the HA, if it has not relayed it earlier;

HA sending the Registration Reply to the FA;

FA then registering the UE in its visitor's cache and forwarding the registration reply to the PDG, if the PDG and the FA are not co-located;

PDG sending IKE_AUTH response that contains AUTH payload;

PDG making AUTH payload with the shared secret derived from EAP authentication procedure and includes the MIP REGISTRATION REPLY;

TSi in the IKE_AUTH message containing the Home Address of the UE as the IP parameter; and

UE obtaining the Home Address from the MIP_REG_REPLY and completes the tunnel establishment procedure.

14. A system for providing mobility and establishing a secure tunnel using IKEv2 messages and MIP messages between the Mobile Node (MN) or user equipment (UE) and the Network Gateway (NGW) wherein the said system comprises of a MN capable of IPsec and MIP procedures, Network Gateway contained in either foreign network or home network, foreign agent collocated with NGW, and a Home Agent in the home network.

15. A method for providing mobility and establishing a secure tunnel using IKEv2 messages and MIP messages between the Mobile Node (MN) or user equipment (UE) and the Network Gateway (NGW) such as herein substantially described particularly with reference to the accompanying drawings.

- 14 -

16. A system for providing mobility and establishing a secure tunnel using IKEv2 messages and MIP messages between the Mobile Node (MN) or user equipment (UE) and the Network Gateway (NGW) such as herein substantially described particularly with reference to the accompanying drawings.

1/3

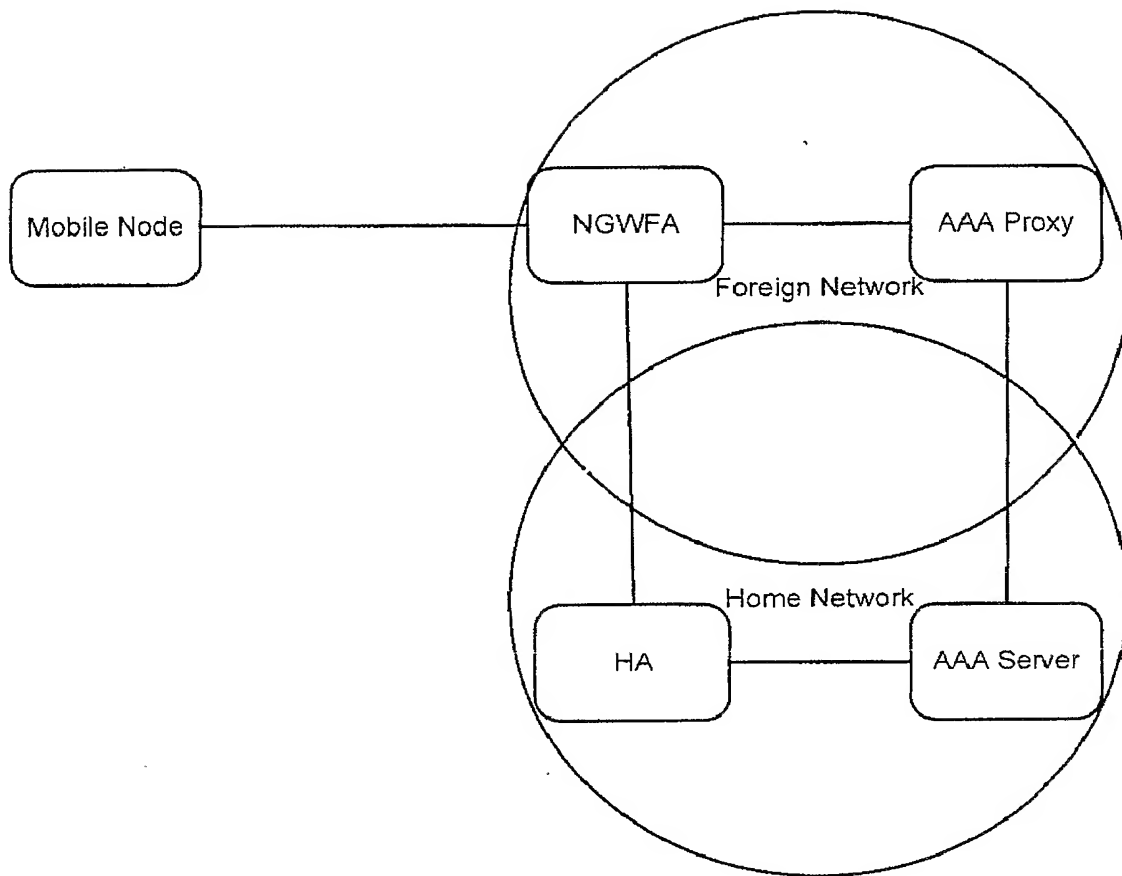


FIG.1

2/3

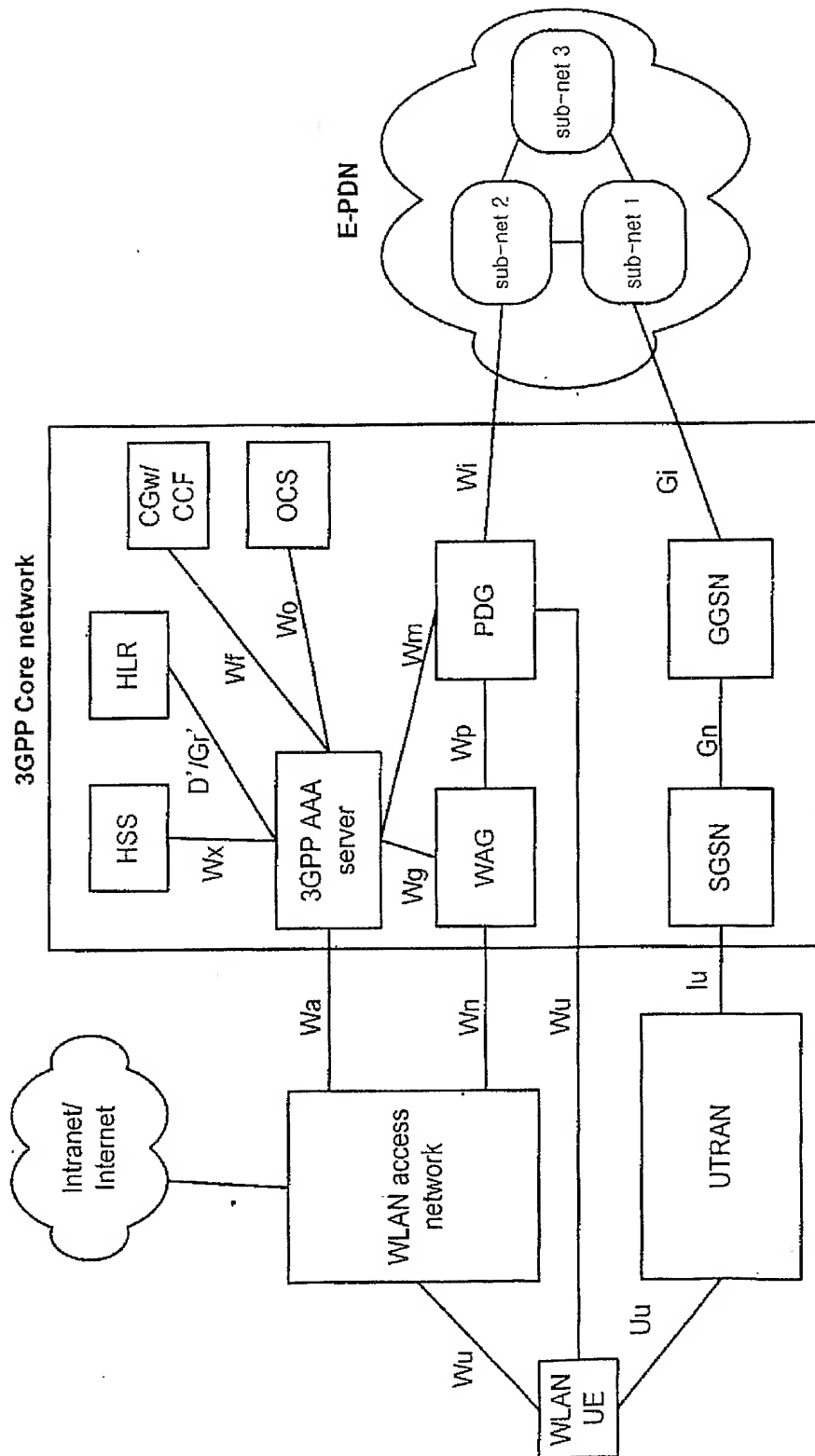


FIG.2

3/3

Procedure for IPSec tunnel setup/Mobility management

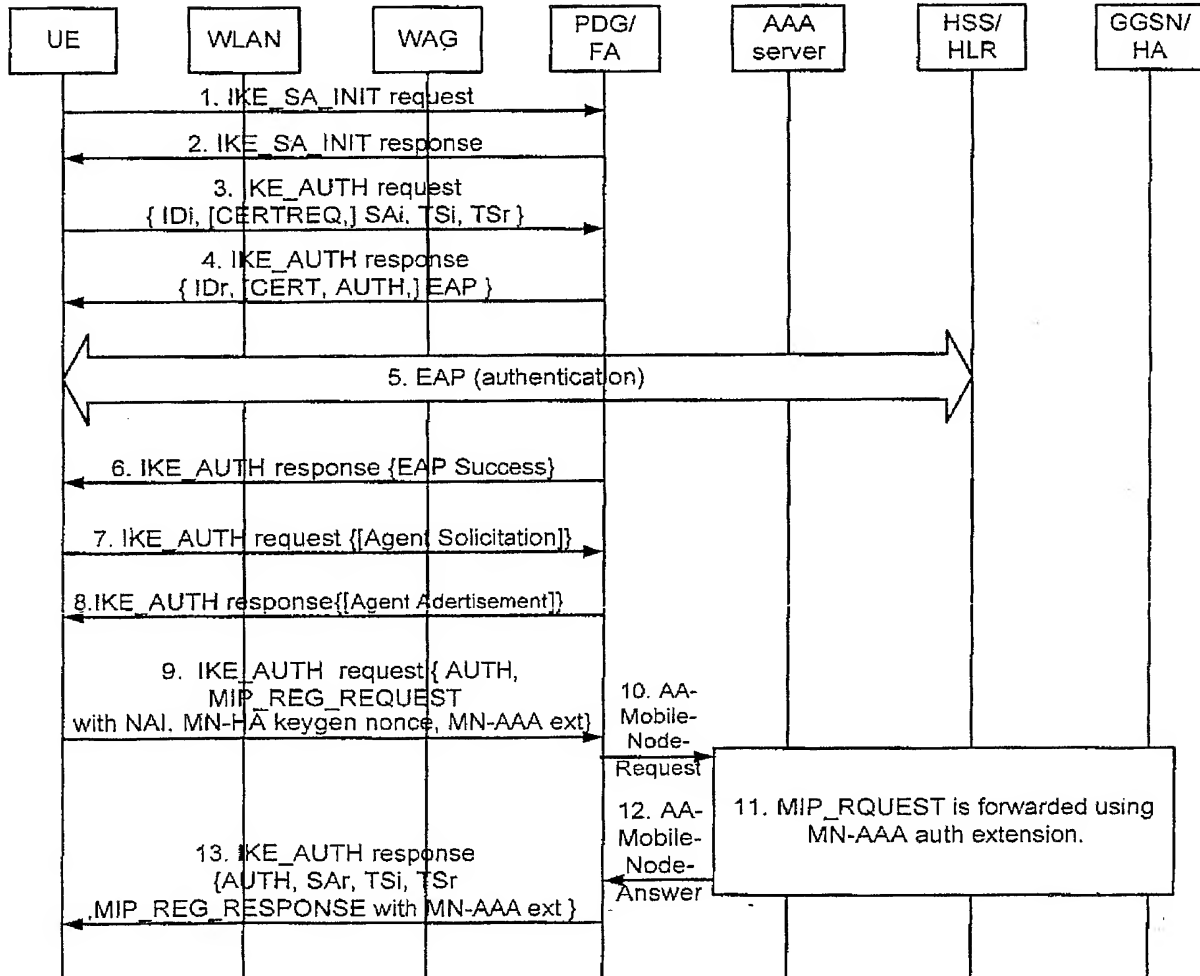


FIG.3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2005/004503**A. CLASSIFICATION OF SUBJECT MATTER****H04B 7/26(2006.01)i**

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC8 H04B 7/26, 7/00, H04L 9/00, G06F 15/16

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

KIPASS, DELPHION, ESPACENET & Keywords : MIP, tunnel, IKE, FA, HA, AAA, IP, IPSec, gateway and similar terms.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US2002-143993 A (SAMSUNG ELECTRONICS CO., LTD.) 3 October 2002 * the whole document *	3,12,13
A	US2004-252653 A (SHIMIZU ET AL.) 16 December 2004 * the whole document *	3,12,13
A	US2002-91921 A (International Business Machines Corporation) 11 July 2002 * abstract, paragraphs[0070]-[0074], figure 11 *	3,12,13



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

31 MARCH 2006 (31.03.2006)

Date of mailing of the international search report

31 MARCH 2006 (31.03.2006)

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
920 Dunsan-dong, Seo-gu, Daejeon 302-701,
Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

KIM, Sang Woo

Telephone No. 82-42-481-8324



INTERNATIONAL SEARCH REPORT

International application No.

PCT/KR2005/004503

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:
2. ☒ Claims Nos.: 1,2,4-11,14-16
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:
 - Claims 1,2,4,14-16 : These claims are only describing a purpose or an effect of the present invention, and suggesting superficial characteristics, thereby not disclosing any technical feature that defines the matter for which protection is sought.
 - Claims 5-11 : These claims are only revealing some parts of the present invention, thereby making the invention incomplete.
3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

- ☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.
- ☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.
- ☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/KR2005/004503

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US2002-143993 A	03. 10. 2002	AU200223148A1	03. 06. 2002
		AU764385B2	14. 08. 2003
		CA2397966A1	30. 05. 2002
		CN1168233C	22. 09. 2004
		CN1395769A	05. 02. 2003
		DE60106549C0	25. 11. 2004
		DE60106549T2	24. 02. 2005
		EP01209875A2	29. 05. 2002
		EP01209875A3	12. 06. 2002
		EP01209875B1	20. 10. 2004
		JP2004515113T2	20. 05. 2004
		KR2002039639A	27. 05. 2002
		W0200243281A1	30. 05. 2002
US2004-252653 A	16. 12. 2004	CN1682498A	12. 10. 2005
		EP01548996A1	29. 06. 2005
		JP2004112011A2	08. 04. 2004
		W02004025908A1	25. 03. 2004
		W02005015245A2	17. 02. 2005
		W02005015245A3	24. 03. 2005
US2002-91921 A	11. 07. 2002	US6931529BB	16. 08. 2005